October 15, 2021

National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899-2000

Submitted via: labeling-eo@nist.gov

RE: Baseline Security Criteria for Consumer Internet of Things (IoT) Devices
Feedback on proposals for a consumer IoT cybersecurity labeling program

Dear NIST IoT Device Labeling Authors:

Infineon Technologies Americas Corp. ("Infineon") designs, develops and manufactures a broad range of semiconductors and system solutions. Our semiconductors enable smart mobility, energy efficiency and secure connectivity. Infineon makes secure chips for credit cards and contactless payment, as well as Trusted Platform Modules ("TPM") which help to secure data on computers and also for connected vehicles, as well as Internet of Things devices ("IoT") devices. Infineon is a long-term, trusted partner of the federal government providing security technology for the e-passport, a leader in international security standards-setting bodies, and works closely with device manufacturers on a variety of hardware-based security solutions. At Infineon, I am the principal lead globally on security for IoT with extensive experience in information security, especially in software and systems. Infineon is pleased to be part of ongoing NIST efforts to better secure the IoT and commends NIST's work to establish the contours of an IoT labeling pilot program I am pleased to provide you feedback on this initiative.

Infineon applauds the goals of Executive Order 14026, Improving the Nation's Cybersecurity, and appreciates the Administration's work across many areas to improve the security of our critical infrastructure. In response to the request for feedback of NIST on a consumer IoT labeling program[1], Infineon commends the use of NISTIR 8259 as the foundation for the program. However, Infineon believes that an appropriate scope for a labeling regime is for a device, rather than the more inclusive proposal of an IoT "product." Looking at the "whole product" from device to cloud and beyond is attractive but problematic. Consumers want to focus on the device that they are buying, and keeping the label tethered to the device would likely be more broadly adopted as this is a voluntary program.

[1] See: https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf

Infineon Technologies Americas Corp.
640 N McCarthy Blvd, Milpitas CA 95035
www.infineon.com

In addition, since the Matter standard[2] permits each device to connect with multiple clouds, the device security must be considered without reference to any particular cloud component. Therefore, it would be difficult to assess the "product" when the cloud can't be known at the point of sale.

Moving to the topic of documentation, Infineon believes that requiring manufacturers to extensively document and publically disclose their development process and security assumptions presents problems, as specific security information is often considered proprietary and confidential information. Public availability of defensive methods and technologies can be used to subvert the very security the federal government is seeking to improve with labeling. Rather than a public disclosure of this nature, that information ought to only be disclosed to the certifying body and strictly protected.

Regarding the discussion of event logging in the proposal, Infineon agrees that it has some security benefits, but it is especially challenging to implement on IoT devices. Low-power devices such as a battery-operated door lock must conserve energy carefully to prolong operations and avoid premature battery replacement or decommission in the case of an item with a fixed battery. Transmitting event logs would be an additional, unbudgeted, power expenditure. In today's smart home, the ability to monitor and analyze these logs does not currently exist. While event logging may be helpful in commercial or government applications, its application across a broad array of IoT products would be harmful to low and extremely low power devices. In Infineon's analysis, this would be an expensive recommendation with little benefit.

The white paper suggests using a short-range network protocol to communicate with insecure components. This presents safety and security concerns in Infineon's reading. With such a design, an attacker could use a high-gain antenna to participate in such a protocol from a long distance, thus the security of the IoT device could be severely impacted. If this approach is adopted, several techniques should be used to decrease this vulnerability. For example, newer versions of protocols -- like Zigbee -- include security features that can protect against such attacks. In addition, lightweight cryptographic algorithms can reduce the burden on low-powered devices.

The white paper says "updating of some product components by [sic] be dependent on or performed by the product component host." Depending on one component to verify updates that are installed in another is believed by Infineon to be dangerous, as illustrated by the Miller and Valasek automotive attack. In that case, the attackers were able to bypass the verification step for a software update by subverting the component responsible for verification. Instead, all updates should be properly authenticated by the component that is installing them. Software update authentication can be

[2] See: buildwithmatter.com

universally deployed throughout the IoT ecosystem at an economical cost, which would eliminate the need for this concept of separate verification.

Infineon supports the concept of IoT labeling and encourages NIST to seek broad and varied approaches to incentivize manufacturer adoption of labels, either by boosting the value of the label or by lowering the cost of obtaining the label. To achieve this, Infineon recommends:

1) Sponsor a broad consumer, industry and retail education initiative. This would include retailers, consumer advocates, device makers, user groups, trade associations, and others, with the goal of educating consumers about the labels and the benefits provided.
2) Leverage the buying power represented by IoT Cybersecurity Improvement Act of 2020, so that all U.S. Government purchases require properly labelled IoT devices.
3) Seek legislative action on creating a limited safe harbor for products that have earned a good rating on their security labels.
4) Expedite the issuance and increase the affordability of labels by incentivizing device maker's use of security certified hardware and software in their designs. Those components have already undergone a rigorous security review by specialized third parties and by their use, the label granting body can be confident that the IoT device including those components meets the necessary security criteria.

Lastly, but important to note, is the structure of the label itself. Carnegie Mellon University research[3] on this topic[4] shows that labels work best when they have both a visual form and a computer-readable form to facilitate automated processing. Infineon respects the work being performed on this topic and encourages its consideration as part of this pilot program.

Thanks again for your work on this important effort. I look forward to participating in finishing this initiative and to its beneficial impact on the IoT marketplace.

Thanks,

Stephen Hanna
Distinguished Engineer, Technical Marketing
Infineon Technologies Americas

[3] https://iotsecurityprivacy.org/
[4] See: https://iotsecurityprivacy.org/research/AskTheExperts